Cited PCT

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 866 613 A1

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
23.09.1998 Bulletin 1998/39

(51) Int. Cl.[6]: **H04N 7/16**, H04N 7/167

(21) Application number: **97402959.7**

(22) Date of filing: **05.12.1997**

(84) Designated Contracting States:
AT BE CH DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE
Designated Extension States:
AL LT LV MK RO SI

(30) Priority: **21.03.1997 EP 97400650**
25.04.1997 WO PCT/FR97/02106

(71) Applicant:
CANAL+ Société Anonyme
75711 Paris Cedex 15 (FR)

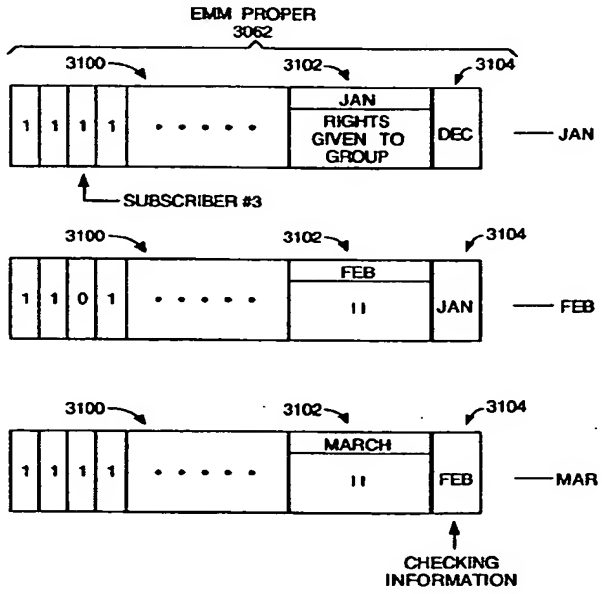
(72) Inventor: **Maillard, Michel**
28130 Maintenon (FR)

(74) Representative:
Cozens, Paul Dennis et al
Mathys & Squire
100 Grays Inn Road
London WC1X 8AL (GB)

(54) Preventing fraudulent access in a conditional access system

(57) A receiver/decoder is programmed only to accept a current entitlement control message (EMM) if it has received at least a previous EMM of a previous calendar period. When this is received, it is used to check present rights in the receiver/decoder. The invention prevents an original subscriber from fraudulently obtaining rights by disconnecting a decoder (before an authorising message can update the decoder's memory to prevent decryption) and by reconnecting the decoder (so as to be mistaken for a new subscriber legitimately having those rights).

Fig.5.



EP 0 866 613 A1

Description

The present invention relates to a method of and apparatus for preventing fraudulent access in a conditional access system linked to a subscriber's receiver/decoder. The technique may be used in the field of data communication where transmitted encrypted data is received and decrypted by, for example, an authorised subscriber's receiver/decoder.

The term "receiver/decoder" used herein may connote a receiver for receiving either encoded or non-encoded signals, for example, television and/or radio signals. The term may also connote a decoder for decoding received signals. Embodiments of such receiver/decoders may include a decoder integral with the receiver for decoding the received signals, for example, in a "set-top box" or such a decoder functioning in combination with a physically separate receiver.

The receiver/decoder is stated above as being "linked to" the conditional access system, which includes the possibilities that the receiver/decoder either forms part of or is separate from the conditional access system.

In particular, but not exclusively, the invention may be used in a mass-market broadcast system having some or all of the following preferred features. It may be an information broadcast system, preferably a radio and/or television broadcast system; it may be a satellite system (although it could be applicable to cable or terrestrial transmission); it may be a digital system, preferably using the MPEG, more preferably the MPEG-2, compression system for data/signal transmission; it may afford the possibility of interactivity; and it may use smartcards. Again, the invention may be used in conjunction with a digital audio visual transmission system. In the context of the present invention the term "digital audio visual transmission system" refers to all transmission systems for transmitting or broadcasting primarily audio visual or multimedia digital data. Whilst the present invention is particularly applicable to a broadcast digital television system, the present invention may equally be used in filtering data sent by a fixed telecommunications network for multimedia internet applications etc.

As used herein, the term "smartcard" includes, but not exclusively so, any chip-based card device possessing, for example, microprocessor and/or memory storage. Also included in this term are chip devices having alternative physical forms, for example key-shaped devices such as are often used in TV decoder systems.

The term MPEG refers to the data transmission standards developed by the International Standards Organisation working group "Motion Pictures Expert Group" and in particular but not exclusively the MPEG-2 standard developed for digital television applications and set out in the documents ISO 13818-1, ISO 13818-2, ISO 13818-3 and ISO 13818-4. In the context of the present patent application, the term includes all variants, modifications or developments of MPEG formats applicable to the field of digital data transmission.

An aim of the invention is to provide a data communication method, transmitter and receiver/decoder which can be used to provide data to, for example, subscribers or other buyers of reception rights on a secure basis.

In existing broadcasting systems, a smartcard is used by a subscriber to obtain the reception right and it has been found pursuant to the present invention that there is a problem of preventing misuse of the card to defraud the owner of the rights.

For example, in a known MPEG television subscriber system, the rights of different subscribers or groups of subscribers can be checked centrally, for instance on a monthly basis, and an authorising message can be subsequently sent, from a central station, to each subscriber or group of subscribers to authorise (or to block) use of the rights. Suitably, the authorising message is simply a "1" or "0" located in different bitmap positions which have been assigned to respective subscriber identities for the month, only the presence of a "1" authorising use of the right for the subscriber at the respective bitmap position, a "0" denying use of that right.

The following problem with this system has been identified pursuant to the present invention. If, for example, the original subscriber ceases payment for the right, after a lapse of time, the system will no longer identify the original subscriber at the previously assigned bitmap position and this position may then be newly assigned to the identity of a "new" subscriber. If the new subscriber has paid for and hence been authorised to use the right, there will be a "1" again in the bitmap position. If, at the "original" subscriber's receiver/decoder, the decoder is disconnected before the next authorising message can update a linked conditional access system (associated with the "original subscriber") and if the decoder is later reconnected (or if a clock is re-set), the "original" subscriber will then be mistaken for the "new" subscriber who has been authorised to use the right and the "original" subscriber will thereby fraudulently obtain the right.

The present invention seeks to solve this problem and other similar or related problems where subscriber rights may be granted over periods of time which may depend typically, but not exclusively, on settling accounts. For example, rights may be granted for considerations other than payment where different subscribers can be authorised to use a system to gain access to a secure area, or to secure information, or to some other secure service.

In the context of the present invention the terms "EMM" and "ECM" are utilised.

An Entitlement Management Message or EMM is a message designated to one subscriber or to a group of subscribers. It is usually generated by a subscription authorisation system and is multiplexed with an MPEG-

2 stream. It is usually encrypted with a so-called "management" key for example for group use. Hence it may be encrypted by a key common to all subscribers in a group of subscribers.

An Entitlement Control Message or ECM is a message sent in relation with one scrambled program. The ECM enables a user to descramble a control word to obtain the right to descramble a television (or similar) programme. A key (termed herein an "ECM key") is passed through the EMM to a subscriber because the smartcard used by the subscriber needs the ECM key to decipher the ECM. The deciphered ECM is used to descramble the control word and hence to descramble the programme.

According to one aspect of the present invention there is provided a method of preventing fraudulent access in a conditional access system which is linked to a subscriber's receiver/decoder for receiving an entitlement management message (EMM) for a group of subscribers to enable said system to provide access for a respective subscriber, the method including the step of:

programming the receiver/decoder only to accept a current EMM of a current calendar period if it has received at least a previous EMM of a previous calendar period.

Hence the problem of preventing fraudulent access can be solved.

The method preferably further comprises the steps of:

transmitting redundant date information with the current EMM; and receiving the current EMM and using redundant date information to check whether said previous EMM has been received.

In a first preferred embodiment, each EMM contains rights date information concerning a current right of access and corresponding check date information concerning a previous right of access, such check date information constituting the redundant date information. This can be a particularly efficient way of putting the invention into practice.

In a second preferred embodiment, the redundant date information is an ECM key of a previous calendar period. This is a convenient alternative way of representing such information.

The subscriber rights may change on a regularly timed basis and the redundant date information may concern an immediately preceding period.

In one illustrative example of the invention, wherein the receiver/decoder is one of a plurality of receiver/decoders in a broadcast system, the subscribers need to have paid for a current month for the right to receive a program or programs and the subscriber rights could change on a monthly basis (since some may not have paid). The bitmap may then be used to indicate the rights for the current month. In this case, when the current EMM is received by the decoder, the redundant date information, e.g. the "previous" ECM key, would be that of the immediately preceding month. However, it is not essential to have sequential periods, since the "current" and "previous" periods may be non-adjacent in time and there could be irregular amounts of real time between such periods. Typically, nonetheless, the previous EMM is for an immediately preceding calendar period, and the periods are sequential.

When there are changes in subscriber rights, it is preferable to include, in the current EMM, a subscriber bitmap having positions representing subscription rights of the subscribers in the group. However, this is unnecessary in situations where all subscribers are authorised, for example, where all subscribers have paid their subscriptions for the respective calendar period; hence this may only occur when there are changes in subscriber rights.

According to another aspect of the invention, there is provided a transmitter for use in a method of preventing fraudulent access in a conditional access system which is linked to a subscriber's receiver/decoder for receiving an entitlement management message (EMM) for a group of subscribers to enable said system to provide access for a respective subscriber, the receiver/decoder being programmed only to accept a current EMM of a current calendar period if it has received at least a previous EMM of a previous calendar period, the transmitter including:

means for transmitting redundant date information with a current EMM of a current calendar period so that the redundant date information can be used by the receiver/decoder to check whether said previous EMM has been received.

Each EMM preferably contains rights date information concerning a current right of access and corresponding check date information concerning a previous right of access, such check date information constituting the redundant date information. Alternatively, the redundant date information may be an ECM key of a previous calendar period.

According to another aspect of the invention, there is provided a receiver/decoder for use in a method of preventing fraudulent access in a conditional access system, the receiver/decoder being linked to the conditional access system and being provided for receiving an entitlement management message (EMM) for a group of subscribers to enable said system to provide access for a respective subscriber, the receiver/decoder including:

means programmed only to accept a current EMM of a current calendar period if it has received at least a previous EMM of a previous calendar period.

14. A receiver/decoder according to Claim 12 or 13 wherein the redundant date information is an ECM key of a previous calendar period.

Fig.1.

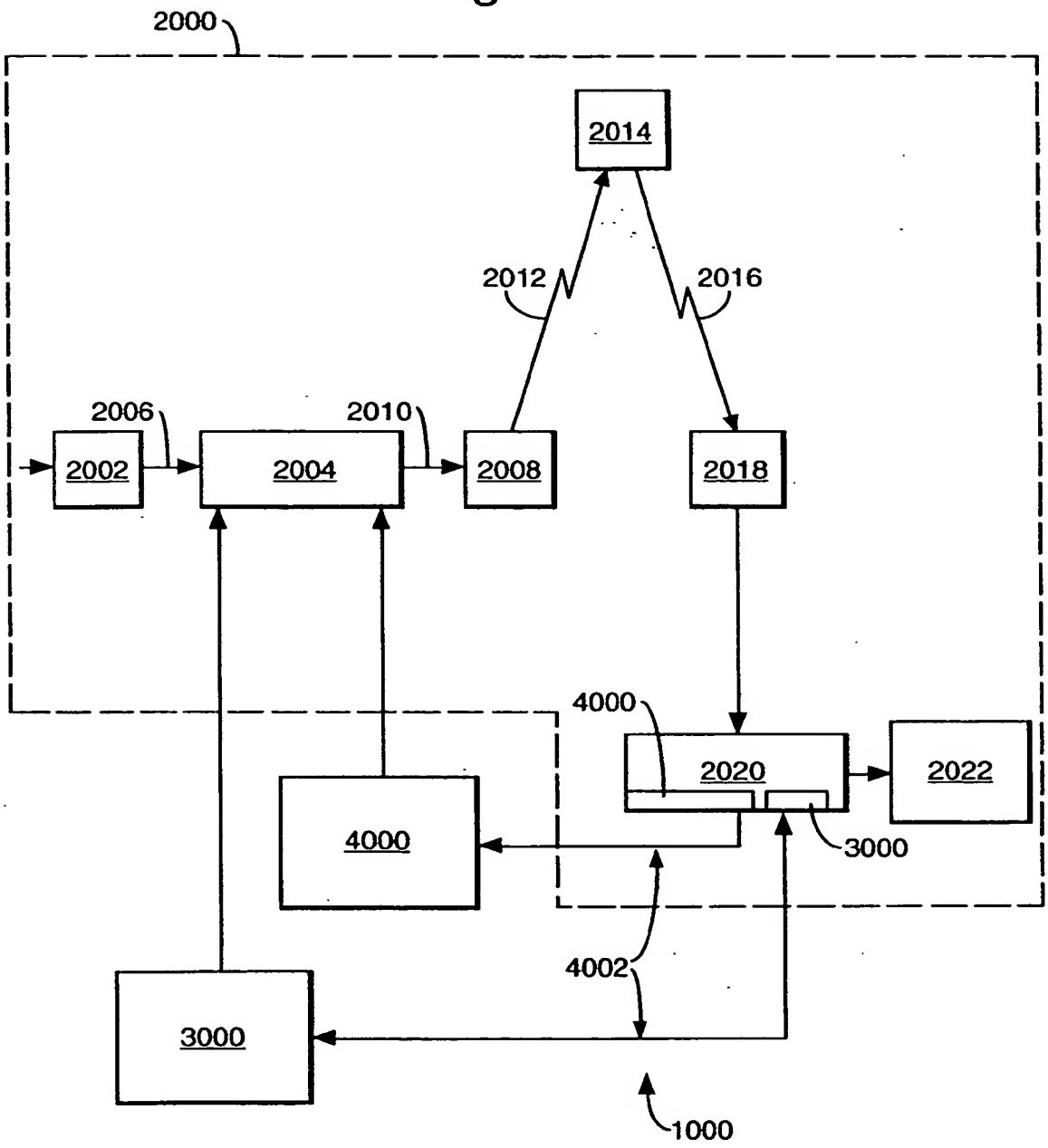


Fig.2.

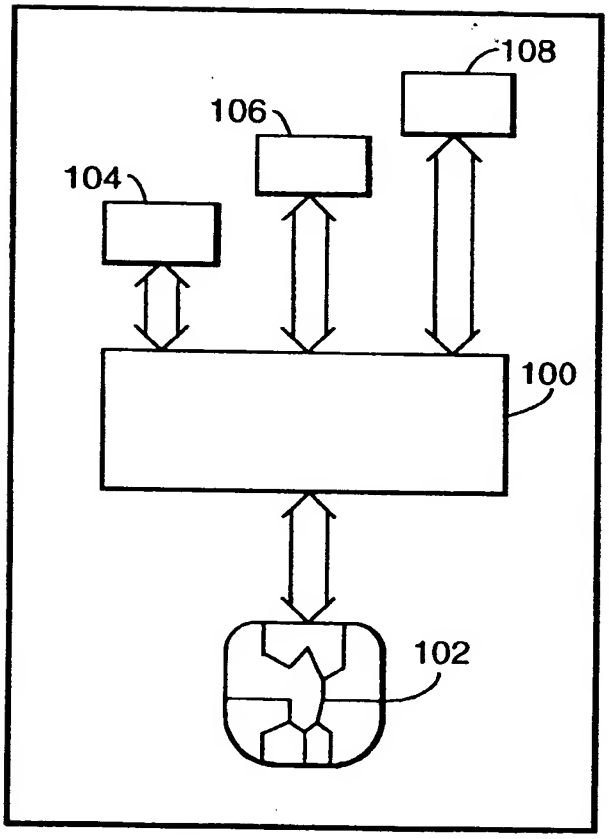


Fig.3.

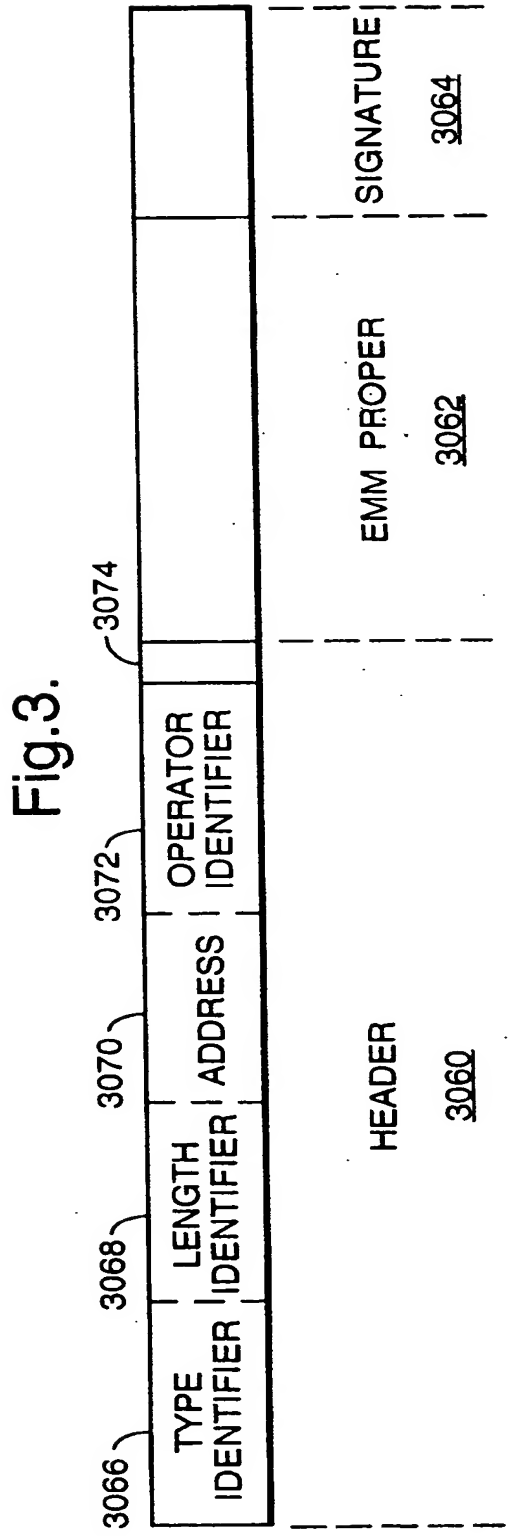


Fig.4.

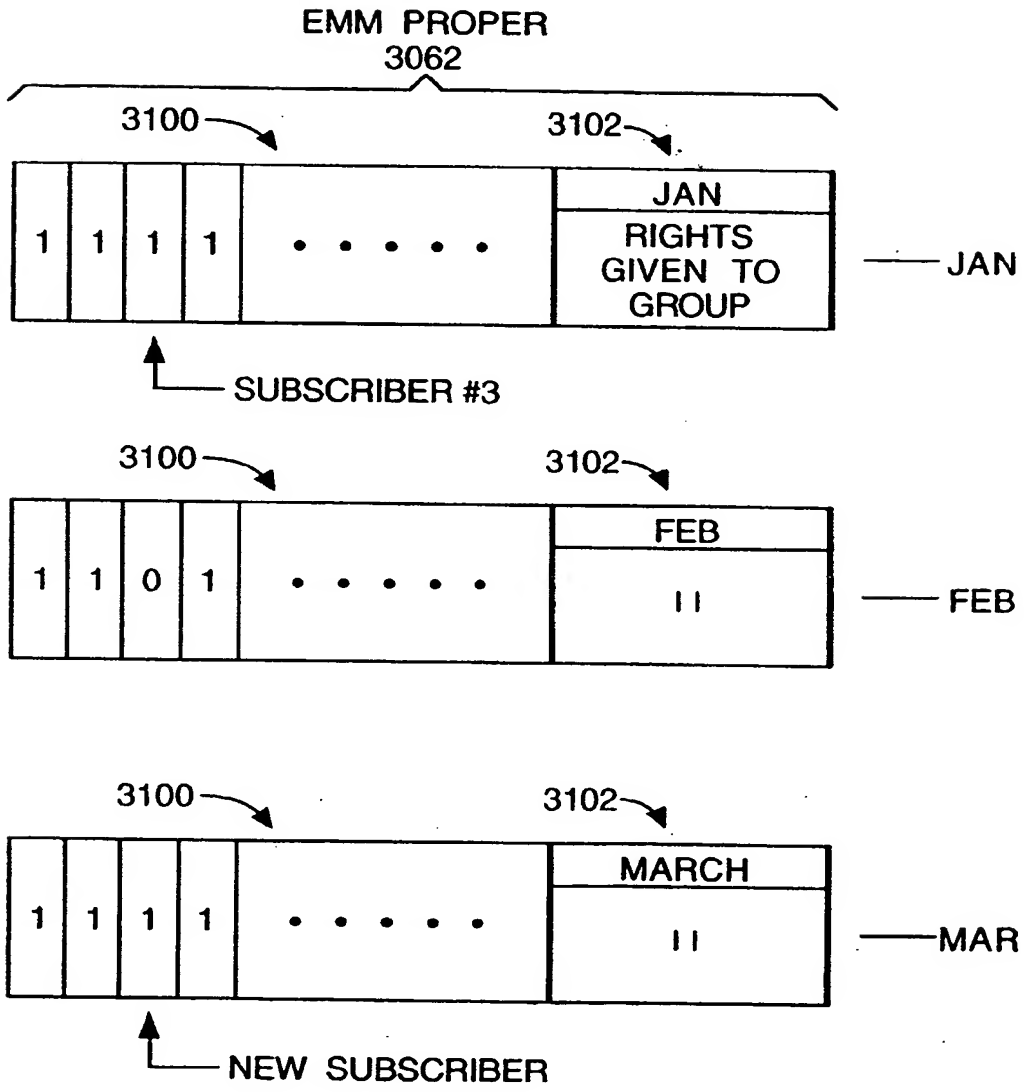


Fig.5.

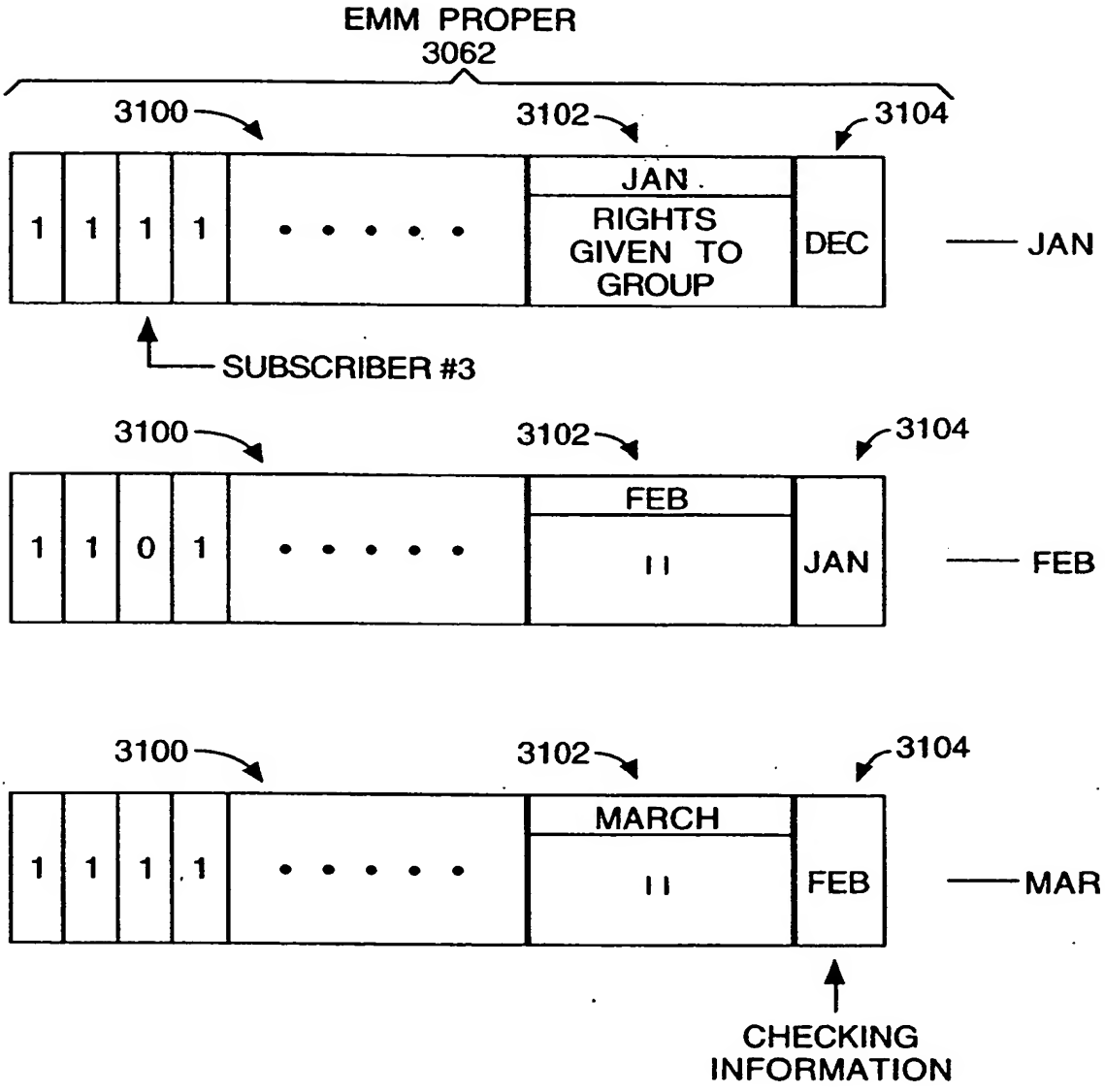


Fig.6.

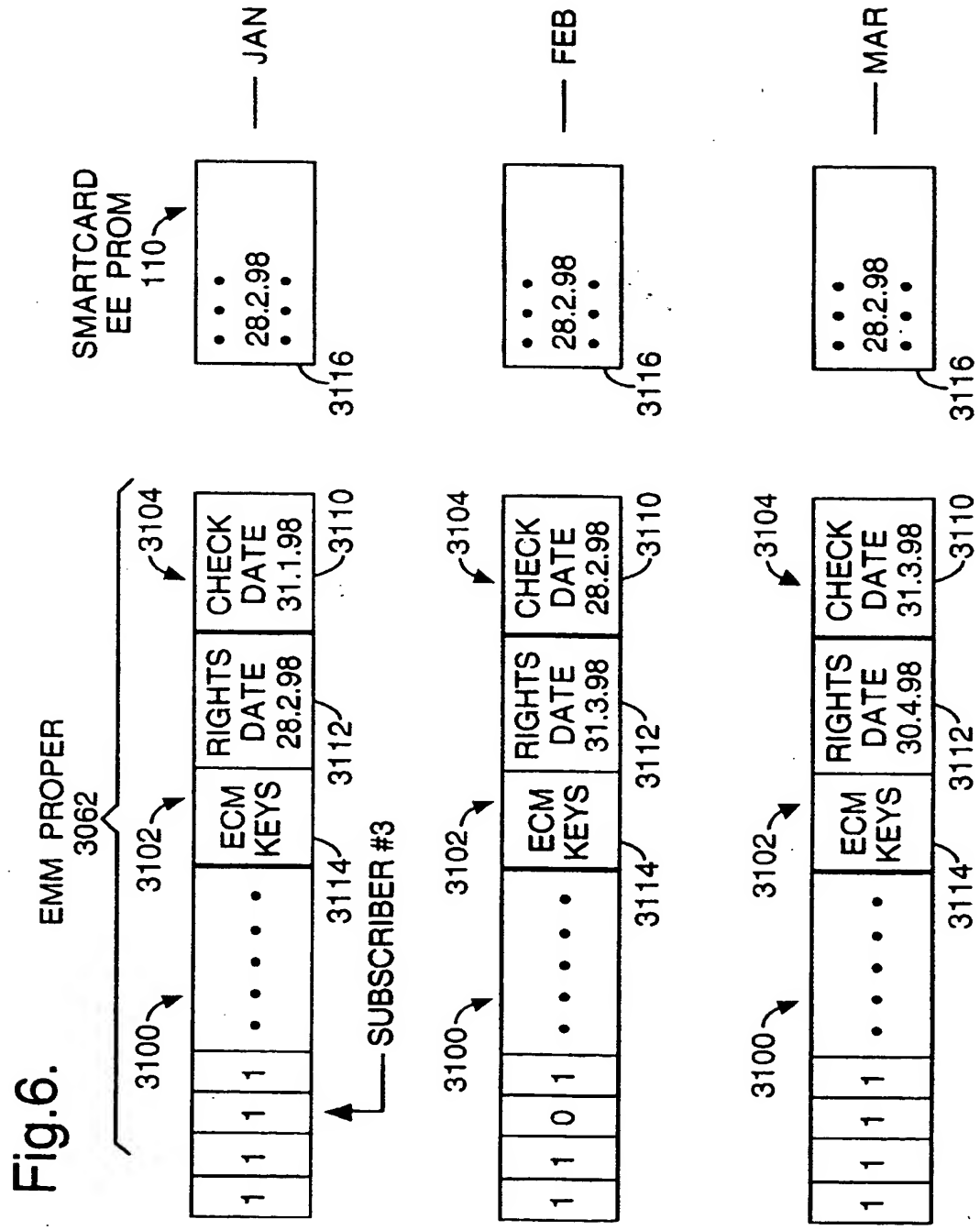


Fig.7.

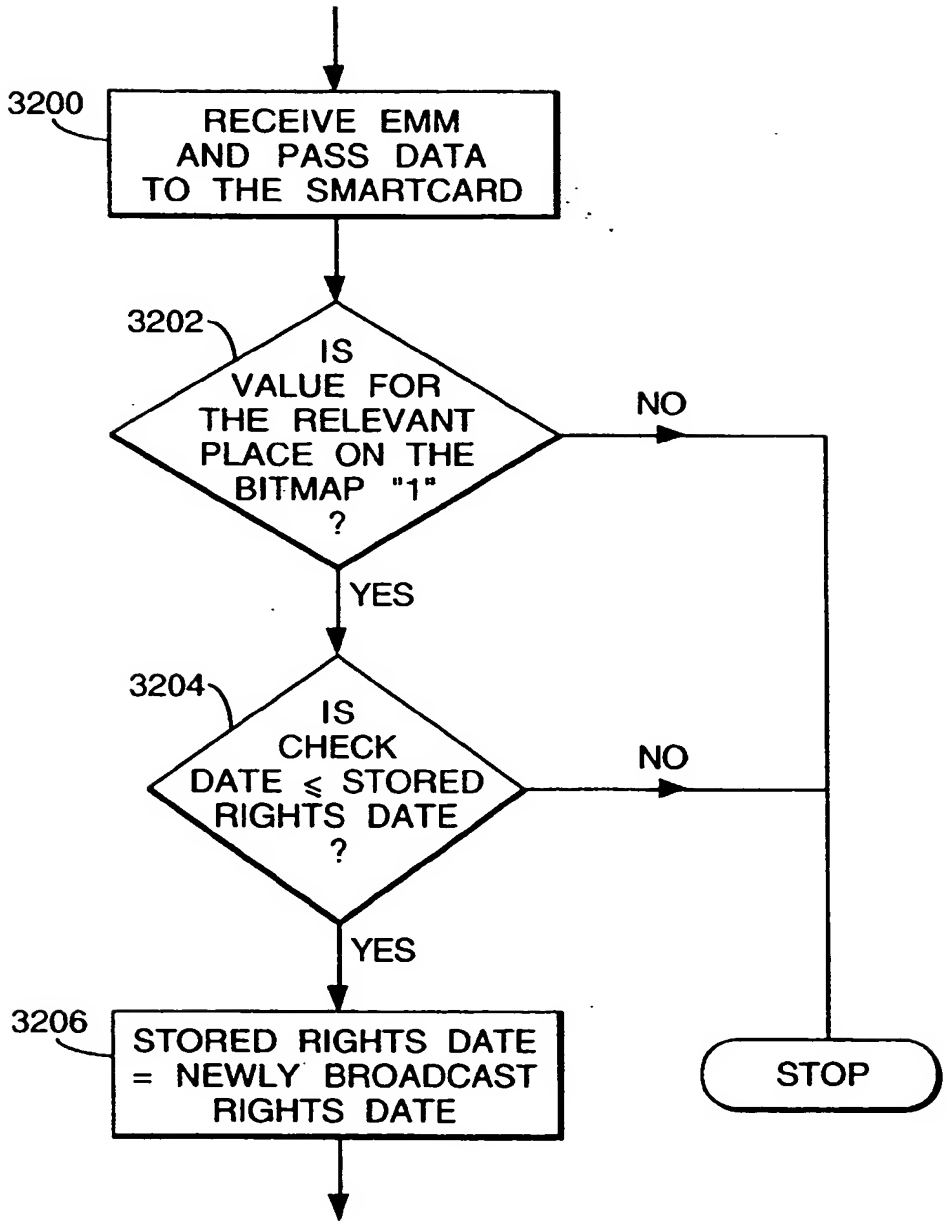
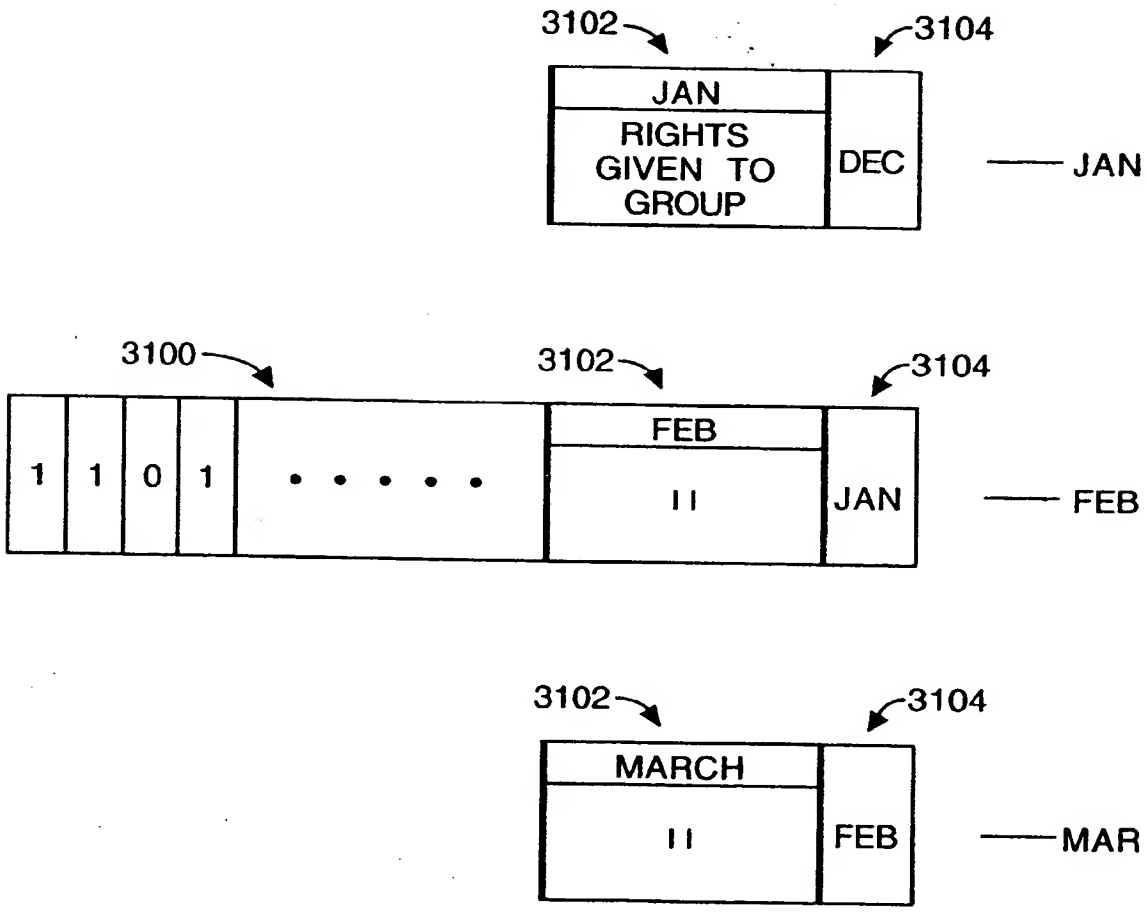


Fig.8.



European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 97 40 2959

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.6)
A	EP 0 763 936 A (LG ELECTRONICS INC) 19 March 1997 * column 16, line 9 - line 46 * * column 24, line 18 - column 25, line 37 * ---	1-14	H04N7/16 H04N7/167
A	WO 85 00718 A (INDEP BROADCASTING AUTHORITY) 14 February 1985 * page 3, line 30 - page 4, line 4 * * page 7, line 23 - line 35 * * page 11, line 1 - page 12, line 15 * ---	1-14	
A	WO 96 06504 A (CHANEY JOHN WILLIAM ;THOMSON CONSUMER ELECTRONICS (US)) 29 February 1996 * page 2, line 11 - line 33 * * page 6, line 11 - line 24 * * page 10, line 3 - line 12 * * page 20, line 8 - line 28 * ---	1-14	
A	WO 95 29560 A (THOMSON CONSUMER ELECTRONICS) 2 November 1995 * page 7, line 17 - page 8, line 32 * ---	1-14	TECHNICAL FIELDS SEARCHED (Int.Cl.6) H04N
A	EP 0 153 837 A (MATSUSHITA ELECTRIC IND CO LTD) 4 September 1985 * page 4, line 22 - page 5, line 8 * ---	1	
A	WO 97 04553 A (PHILIPS ELECTRONICS NV ;PHILIPS NORDEN AB (SE)) 6 February 1997 ---		
A	EP 0 723 371 A (THOMSON MULTIMEDIA SA) 24 July 1996 -----		

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
THE HAGUE	30 July 1998	Poirier, J-M

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

Fig.1.

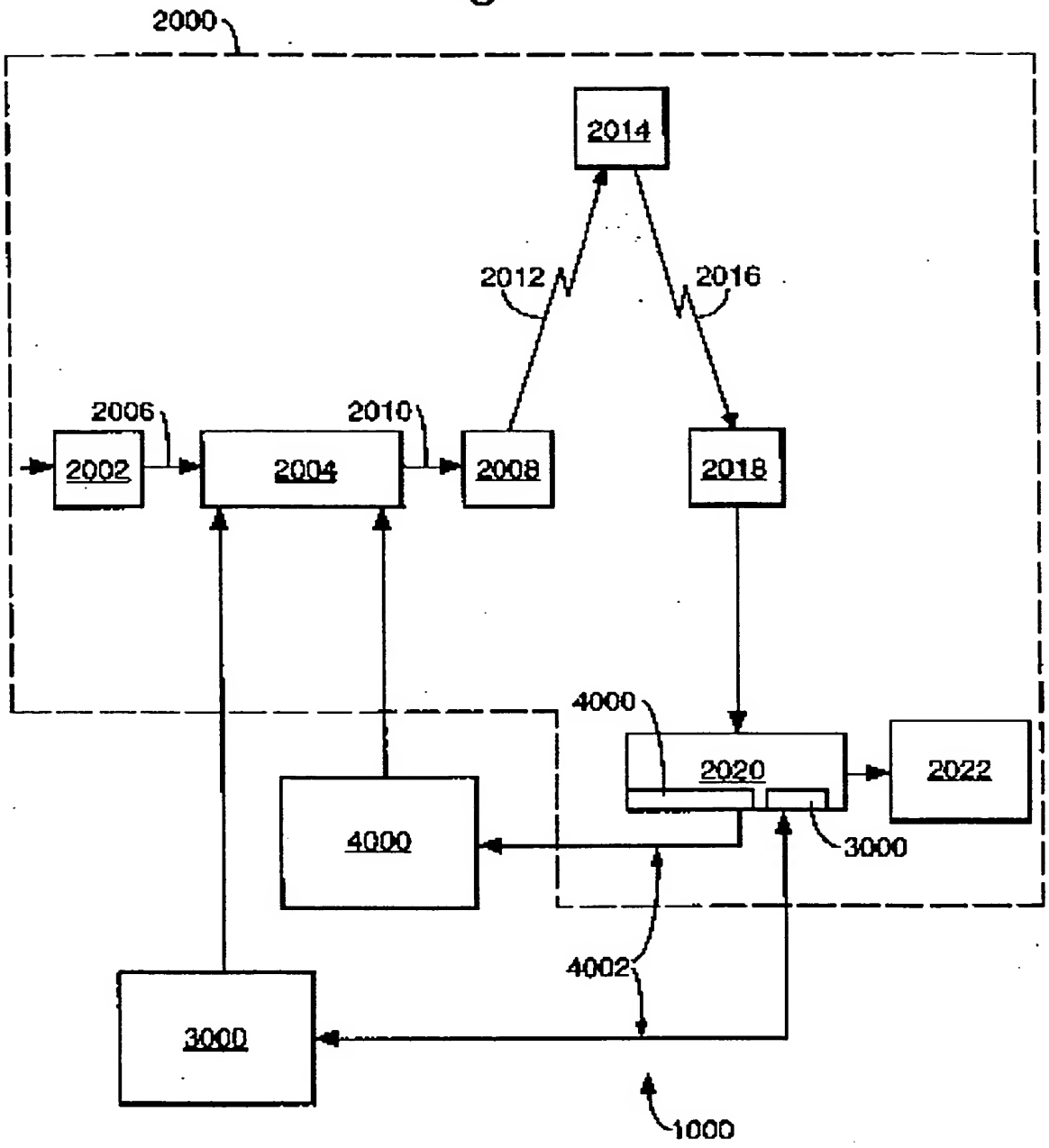


Fig.2.

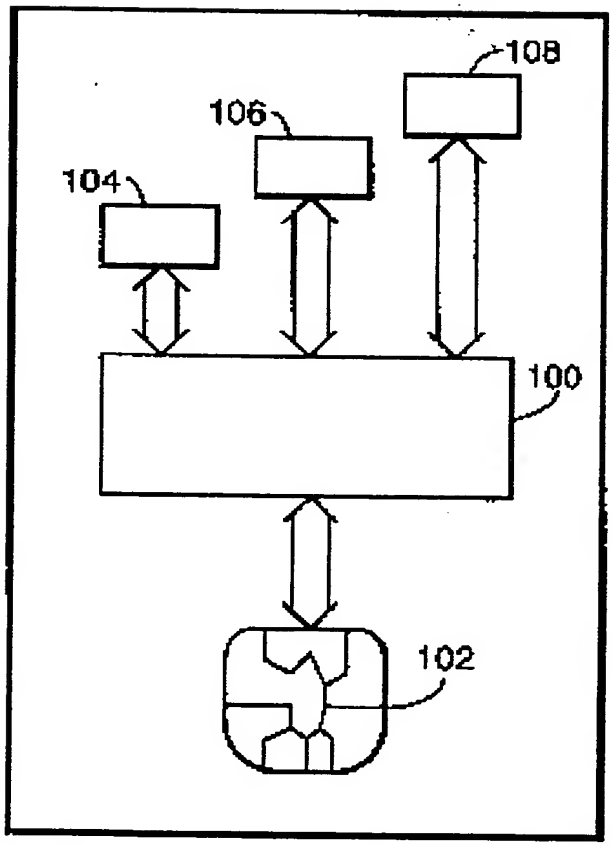


Fig.3.

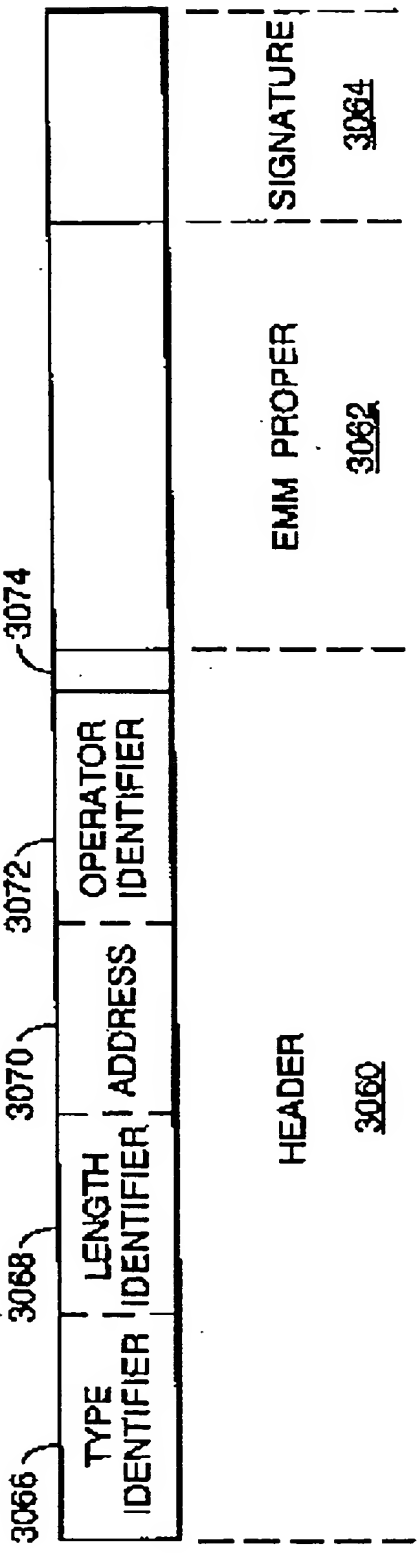


Fig.4.

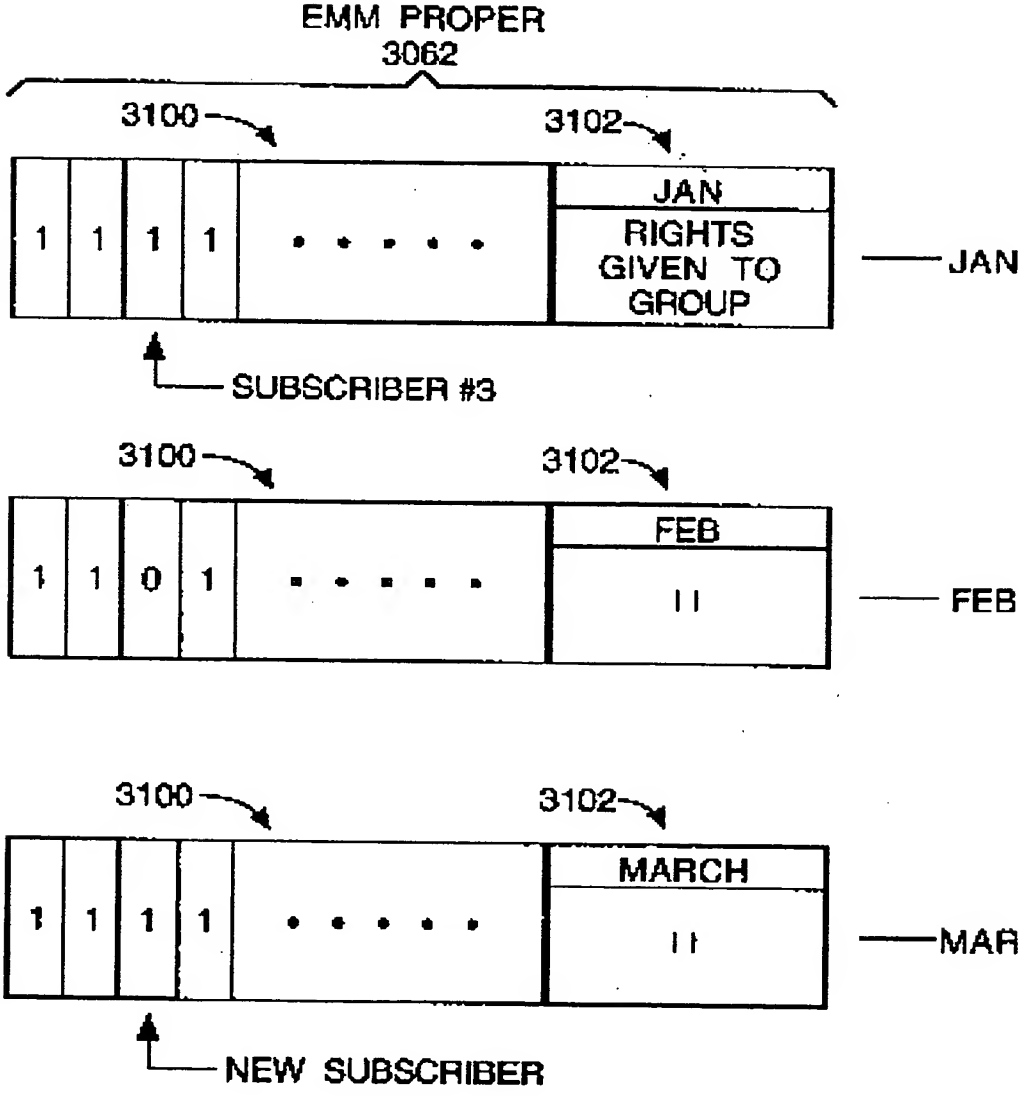


Fig.5.

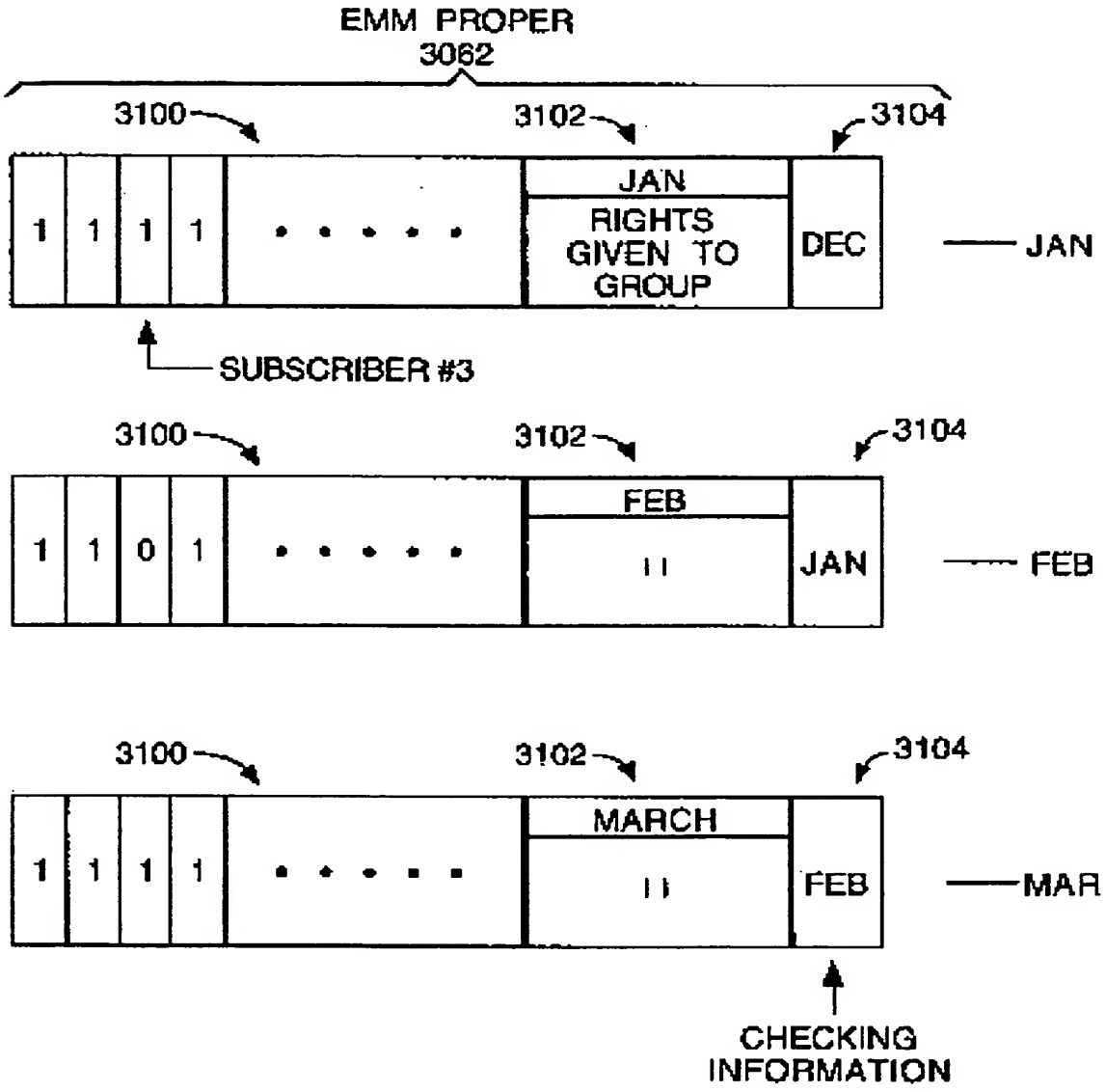


Fig.6.

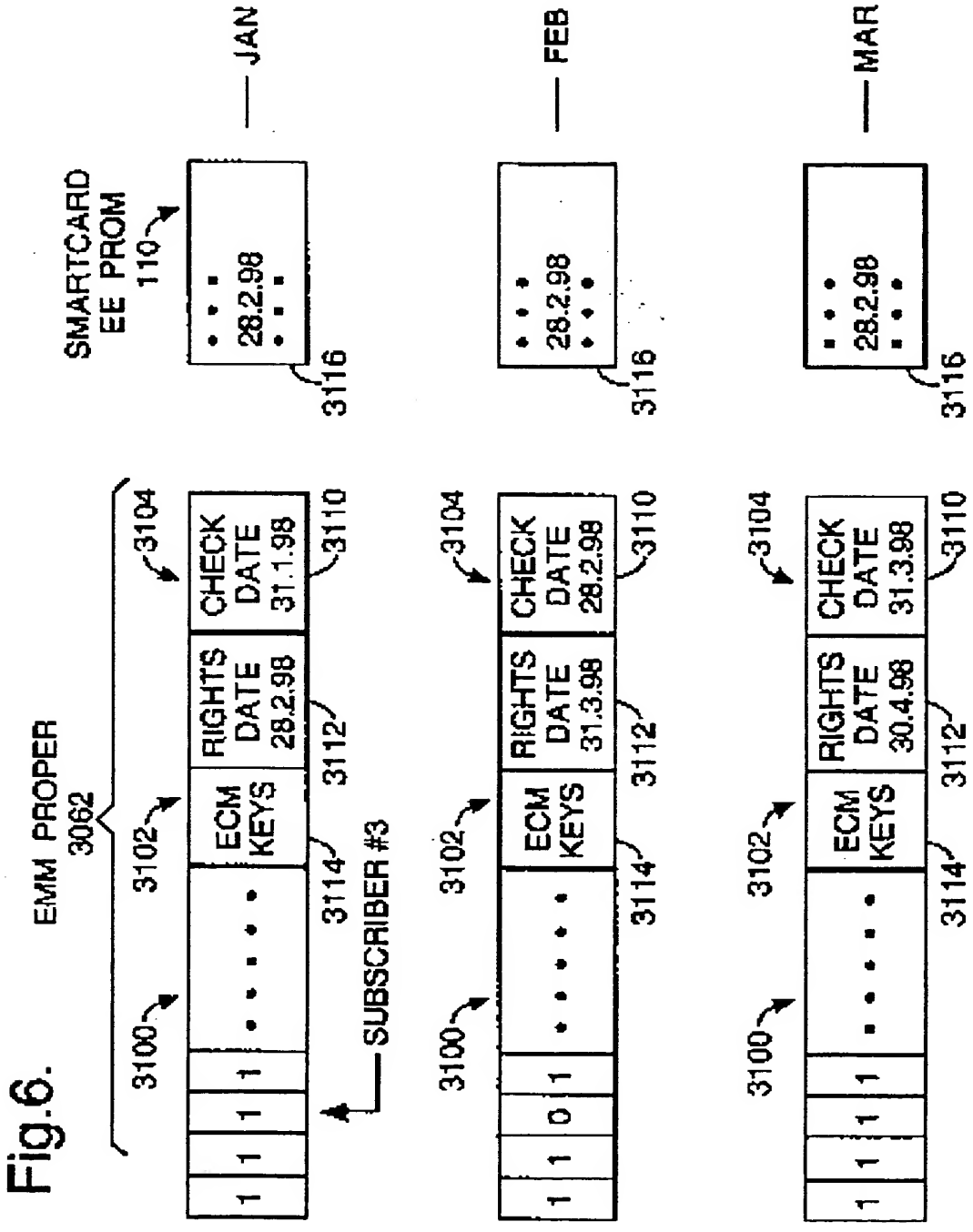


Fig.7.

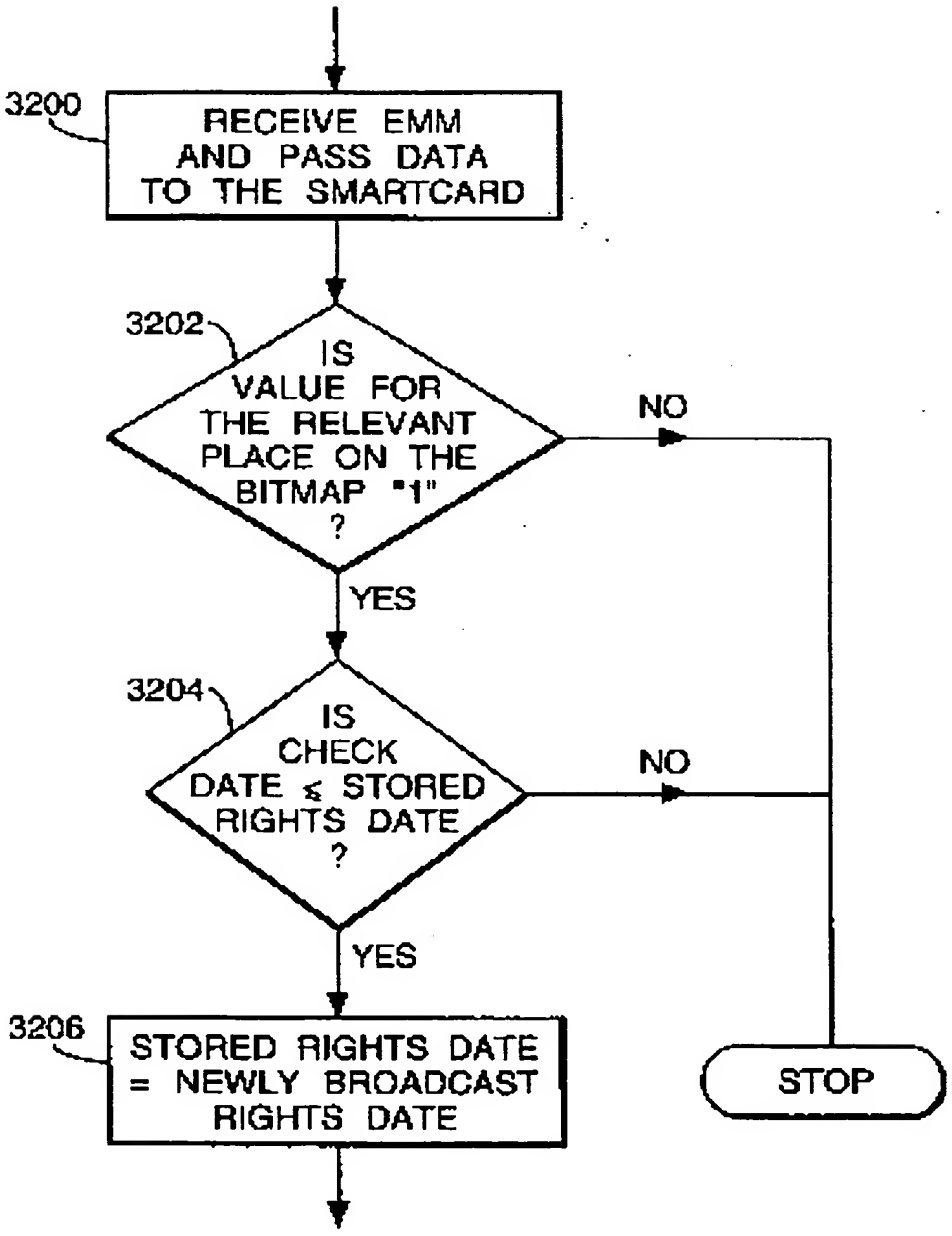


Fig.8.